UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,729	10/12/2001	Ralf Dohmen	9-1-4-9	2459

7590 01/20/2004

Ryan, Mason & Lewis, LLP
Suite 205
1300 Post Road
Fairfield, CT 06430

EXAMINER	
TORRES, JOSEPH D	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 01/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/976,729	DOHMEN ET AL.	
	Examiner	Art Unit	
	Joseph D. Torres	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) *15-18 and 20-24* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14 and 19* is/are rejected.

7)☒ Claim(s) *1-14 and 19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 February 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

   I. Claims 1-14 and 19, drawn to Sixteen Three-Parallel Syndrome Generators whereby Four Three-Parallel Syndrome Generators Share a Single Key Equation Determination Device out of Four Key Equation Determination Devices, classified in class 714, subclass 785.

   II. Claims 15-18, drawn to Parallel Generation of Parity Bits, classified in class 714, subclass 757.

   III. Claims 20-24, drawn to A Retransmission Circuit with and Decoder coupled Encoder for Error Correction Decoding, Error Correction Re-Encoding and Re-Transmitting, classified in class 714, subclass 776.

The inventions are distinct, each from the other because of the following reasons: Inventions Group I, Sixteen Three-Parallel Syndrome Generators whereby Four Three-Parallel Syndrome Generators Share a Single Key Equation Determination Device out of Four Key Equation Determination Devices, and Group II, Parallel Generation of Parity Bits, are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention Group I, Sixteen Three-Parallel Syndrome Generators whereby Four Three-Parallel Syndrome Generators Share a

Single Key Equation Determination Device out of Four Key Equation Determination Devices, and Group II, Parallel Generation of Parity Bits, has separate utility such as for use with Reed-Solomon or BCH codes. In the instant case, invention Group II, Parallel Generation of Parity Bits, has separate utility such as general parity codes, for example, Hamming codes, which do not require the specifics of claims 1-14, and 19 for decoding. See MPEP § 806.05(d).

Inventions Group III, A Retransmission Circuit with and Decoder coupled Encoder for Error Correction Decoding, Error Correction Re-Encoding and Re-Transmitting, and Group I, Sixteen Three-Parallel Syndrome Generators whereby Four Three-Parallel Syndrome Generators Share a Single Key Equation Determination Device out of Four Key Equation Determination Devices, are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination, Group III A Retransmission Circuit with and Decoder coupled Encoder for Error Correction Decoding, Error Correction Re-Encoding and Re-Transmitting, as claimed does not require the particulars of the subcombination, Group I Sixteen Three-Parallel Syndrome Generators whereby Four Three-Parallel Syndrome Generators Share a Single Key Equation Determination Device out of Four Key Equation Determination Devices, as claimed because Error correction for Reed Solomon or BCH codes does not require

sixteen three-parallel syndrome generators whereby four three-parallel syndrome generators share a single key equation determination device out of four key equation determination devices. The subcombination has separate utility such as in specific applications requiring sixteen three-parallel syndrome generators whereby four three-parallel syndrome generators share a single key equation determination device out of four key equation determination devices.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Group II and vice-a-versa, restriction for examination purposes as indicated is proper.

Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Group III and vice-a-versa, restriction for examination purposes as indicated is proper.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

During a telephone conversation with Robert J. Mauri on 7 January 2004 a provisional election was made with traverse to prosecute the invention of Group I, claims 1-14 and

19. Affirmation of this election must be made by applicant in replying to this Office action. Claims 15-18 and 20-24 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Information Disclosure Statement

The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609 A(1) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

In particular, the Examiner requires that the Applicant provide a copy of the Mastrovito paper (Mastrovito, "VLSI designs for multiplication over finite fields GF(2.sup.m)," Int'l Conf. on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, 297-309, Rome, July 1988 paper) cited on lines 10-15 of page 28 of the Applicant's specification.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: '220'. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: '375' in Figure 3. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "470" in Figure 3 has been used to designate the same signal line. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

3. Claims 1-14 and 19 are objected to because of the following informalities: claim 1 recites, "a plurality of N-parallel syndrome generators, each of the N-parallel syndrome generators coupled to a parallel data stream and being adapted to perform a calculation each cycle with N symbols". The Examiner asserts that a plurality of N-parallel syndrome generators operating in parallel is just a plurality of parallel syndrome generators, for example k N-parallel syndrome generators, whereby each of the N-parallel syndrome generators is coupled to a parallel data stream and is adapted to perform a calculation each cycle with N symbols, is kxN parallel syndrome generators adapted to perform a calculation each cycle with kxN symbols.

Claims 2-14 depend from claim 1, hence inherit the deficiencies in claim 1.

Claim 19 recites similar language as in claim 1.

Clarification is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "N-parallel generators" in line 6. There is insufficient antecedent basis for this limitation in the claim.

Claim 1 recites, "adapted to use the at least one error polynomial". Since the term "adapted" leaves optional the "use the at least one error polynomial", it is not clear whether the "at least one error polynomial" is used, which renders the claim language indefinite.

Clams 3, 4, 6, 7 and 8 all use the term "adapted" in a similar manner.

Claims 2-14 depend from claim 1, hence inherit the deficiencies in claim 1.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-3 are rejected under 35 U.S.C. 102(e) as being anticipated by Chen, Yen-Hao (US 6571368 B1).

35 U.S.C. 102(e) rejection of claim 1.

Chen teaches a decoder (the decoder in Figure 6 of Chen is a parallel decoder) comprising: a plurality of N-parallel syndrome generators (Figure 6 of Chen teaches a plurality k of N-parallel syndrome generators, i.e. 2t+1= kxN syndrome generators;

Note: a plurality of N-parallel syndrome generators operating in parallel is just a plurality

of parallel syndrome generators, for example k N-parallel syndrome generators, whereby each of the N-parallel syndrome generators is coupled to a parallel data stream and is adapted to perform a calculation each cycle with N symbols, is kxN parallel syndrome generators adapted to perform a calculation each cycle with kxN symbols), each of the N-parallel syndrome generators coupled to a parallel data stream and being adapted to perform a calculation each cycle with N symbols from the parallel data stream (Figure 6 in Chen teaches N parallel syndrome generators, S_0, S_1... S_{2t}, coupled to a parallel data stream and being adapted to perform a calculation each cycle with N=2t+1 symbols from the parallel data stream, see col. 9, lines 3-6 in Chen); a plurality of key equation determination devices (Row F in Figure 6 of Chen comprises key equation computation cells, f_0, f_1... f_{2t}, for applying Euclid's algorithm for generating error locator and error value polynomials, see col. 9, lines 10-14 in Chen), each key equation determination device coupled to at least one of the N-parallel generators and being adapted to determine at least one error polynomial (Figure 6 in Chen teaches that each key equation determination device, f_0, f_1... f_{2t}, is coupled to at least one of the N-parallel generators, S_0, S_1... S_{2t}, and is adapted to determine at least one error polynomial, see col. 4, lines 28-29 of Chen); and a plurality of N-parallel error determination and correcting devices, one for each of the N-parallel syndrome generators, each N-parallel error correction and determination device coupled to one of the key equation determination devices and being adapted to use the at least one error polynomial produced by the one key equation determination device to correct errors in the parallel data stream (row E:G, H and Ω_Λ in Figure 6 of Chen comprises N-parallel

error determination and correcting devices, one for each of the N-parallel syndrome generators, S_0, S_1... S_{2t}, each N-parallel error correction and determination device coupled to one of the key equation determination devices, f_0, f_1... f_{2t}, and being adapted to use the at least one error polynomial produced by the one key equation determination device, f_0, f_1... f_{2t}, to correct errors in the parallel data stream; Note: 515 and 516 in Figure 5 of Chen teach that the results of the Array Decoder in Figure 6 of Chen are used to correct errors in the parallel data stream).

35 U.S.C. 102(e) rejection of claim 2.

kxN=2t+1 in Figure 6 where k is the plurality of N-parallel syndrome generators. If t=4, then N=3 when k=3; hence N=3 corresponds to a 4 error correcting code which is clearly taught and encompassed by the Chen patent.

35 U.S.C. 102(e) rejection of claim 3.

Col. 2, lines 45-50 in Chen teach the input to the syndrome generator is a serial input and Figure 6 of Chen teaches that the serial input is converted to a parallel data stream.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

6. Claims 4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, Yen-Hao (US 6571368 B1) in view of Yun, Young-Han (US 5526368 A).

35 U.S.C. 103(a) rejection of claim 4.

Chen, substantially teaches the claimed invention described in claims 1-3 (as rejected above).

However Chen does not explicitly teach the specific use of a method for determining the number of codewords with uncorrectable errors.

Yun, in an analogous art, teaches a method for determining the number of codewords with uncorrectable errors for use in an error correcting decision process (col. 10, lines 48-51, Yun).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Chen with the teachings of Yun by including use of a method for determining the number of codewords with uncorrectable errors. This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that

use of a method for determining the number of codewords with uncorrectable errors would have provided the opportunity to use the number of codewords with uncorrectable errors in an error correcting decision process (col. 10, lines 48-51, Yun).

35 U.S.C. 103(a) rejection of claim 6.

Chen, substantially teaches the claimed invention described in claims 1-3 (as rejected above). In addition, the device of Figure 5 and 6 in Chen is a device for oututing a number of corrected bit errors.

However Chen does not explicitly teach the specific use of a plurality of codewords in a frame.

Yun, in an analogous art, teaches use of a plurality of codewords in a frame (see Figure 2 in Yun). Note: Chen teaches error correction which is a means for maintaining an acceptable degree of data integrity for data communications. One of ordinary skill in the art at the time the invention was made would have been highly motivated to combine the teachings in the Chen patent with the teachings in the Yun patent to provide an acceptable degree of data integrity in commonly used data packet/frame protocols as presented in the Yun patent since data packet/frame protocols are communications protocols.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Chen with the teachings of Yun by including use of a plurality of codewords in a frame. This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill

in the art would have recognized that use of a plurality of codewords in a frame would have provided the opportunity to guarantee an acceptable degree of data integrity in commonly used data packet/frame protocols as presented in the Yun patent since data packet/frame protocols are communications protocols.

7. Claims 8, 9 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, Yen-Hao (US 6571368 B1) in view of White, Philip E. (US 5754563 A).

35 U.S.C. 103(a) rejection of claim 8.

Chen, substantially teaches the claimed invention described in claims 1-3 (as rejected above).

However Chen, does not explicitly teach the specific use of parallel correction of data.

The Examiner asserts that Chen teaches error correction circuitry for extracting key equations in parallel for use in error correction circuitry 515 in Figure 5 of Chen to create a data stream E(x) of correction values indicating a position in the second parallel data stream at which an error occurs. However, Chen does not teach that E(x) is a parallel data stream since the novelty in the Chen patent is the implementation of Error Correction Circuitry 511-515 in parallel. White on the other hand teaches the use of implementing a Most Likely Code Word Generator 308 in Figures 3, 7 and 7-A which takes data from Error Correction Circuitry 511-515 as taught in the Chen patent in parallel whereby c(x) is a parallel data stream comprising corrected symbols and e(x) is a parallel stream of correction values, each bit in the parallel stream of correction values

indicating a position in the second parallel data stream at which an error occurs. One of ordinary skill in the art at the time the invention was made would have been highly motivated to combine the teachings in Chen patent with the teachings in White patent to achieve high speed circuitry throughout the required error correction processing in the Chen and white patents (see Abstract, White).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Chen with the teachings of White by including use of parallel correction of data. This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that use of parallel correction of data would have provided the opportunity to achieve high speed circuitry throughout the required error correction processing in the Chen and white patents (see Abstract, White).

35 U.S.C. 103(a) rejection of claim 9.

Feedback Failure Location System 400 in Figure 1 of White is a peripheral performing error analyses using the parallel stream of correction values.

35 U.S.C. 103(a) rejection of claim 19.

Chen teaches converting a serial input data stream into a parallel data stream (col. 2, lines 45-50 in Chen teach the input to the syndrome generator is a serial input and Figure 6 of Chen teaches that the serial input is converted to a parallel data stream); performing, in parallel, a plurality of N-parallel decodings of the parallel data stream to

determine, in parallel, a plurality of error value and error locator polynomials (Figure 6 of Chen of Chen teaches a plurality k of N-parallel syndrome generators, i.e. 2t+1= kxN syndrome generators; Note: a plurality of N-parallel syndrome generators operating in parallel is just a plurality of parallel syndrome generators, for example k N-parallel syndrome generators, whereby each of the N-parallel syndrome generators is coupled to a parallel data stream and is adapted to perform a calculation each cycle with N symbols, is kxN parallel syndrome generators adapted to perform a calculation each cycle with kxN symbols; Figure 6 in Chen teaches N parallel syndrome generators, S_0, $S_1 \ldots S_{2t}$, coupled to a parallel data stream and being adapted to perform a calculation each cycle with N=2t+1 symbols from the parallel data stream, see col. 9, lines 3-6 in Chen; Row F in Figure 6 of Chen comprises key equation computation cells, f_0, $f_1 \ldots f_{2t}$, for applying Euclid's algorithm for generating error locator and error value polynomials, see col. 9, lines 10-14 in Chen); and correcting errors, by using a plurality of N-parallel correction and determination processes that use the error value and error locator polynomials, in the parallel data stream (row E:G, H and Ω_Λ in Figure 6 of Chen comprises N-parallel error determination and correcting devices, one for each of the N-parallel syndrome generators, S_0, $S_1 \ldots S_{2t}$, each N-parallel error correction and determination device coupled to one of the key equation determination devices, f_0, $f_1 \ldots f_{2t}$, and being adapted to use the at least one error polynomial produced by the one key equation determination device, f_0, $f_1 \ldots f_{2t}$, to correct errors in the parallel data stream; Note: 515 and 516 in Figure 5 of Chen teach that the results of the Array Decoder in Figure 6 of Chen are used to correct errors in the parallel data stream).

However Chen, does not explicitly teach the specific use of parallel correction of data. The Examiner asserts that Chen teaches error correction circuitry for extracting key equation in parallel for use in error correction circuitry 515 in Figure 5 of Chen to create a data stream E(x) of correction values indicating a position in the second parallel data stream at which an error occurs. However, Chen does not teach that E(x) is a parallel data stream since the novelty in the Chen patent is the implementation of Error Correction Circuitry 511-515 in parallel. White on the other hand teaches the use of implementing a Most Likely Code Word Generator 308 in Figures 3, 7 and 7-A which takes data from Error Correction Circuitry 511-515 as taught in the Chen patent in parallel whereby c(x) is a parallel data stream comprising corrected symbols and e(x) is a parallel stream of correction values, each bit in the parallel stream of correction values indicating a position in the second parallel data stream at which an error occurs. One of ordinary skill in the art at the time the invention was made would have been highly motivated to combine the teachings in Chen patent with the teachings in White patent to achieve high speed circuitry throughout the required error correction processing in the Chen and white patents (see Abstract, White).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Chen with the teachings of White by including use of parallel correction of data. This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that use of parallel correction of data would have

provided the opportunity to achieve high speed circuitry throughout the required error correction processing in the Chen and white patents (see Abstract, White).

8. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, Yen-Hao (US 6571368 B1) in view of Mastrovito (Mastrovito, "VLSI designs for multiplication over finite fields GF(2.sup.m)," Int'l Conf. on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, 297-309, Rome, July 1988).

35 U.S.C. 103(a) rejection of claim 10.

Chen, substantially teaches the claimed invention described in claims 1-3 (as rejected above).

However Chen, does not explicitly teach the specific use of Mastrovito standard-basis multiplier.

The Applicant admits on lines 10-15 of page 28 of the Applicant's specification that the Mastrovito standard-basis multiplier is a composite-basis multiplier over finite fields $GF(2^m)$ with reduced complexity and higher speed (lines 16-18 of page 31 of the Applicant's specification).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Chen with the teachings of Mastrovito by including use of Mastrovito standard-basis multiplier. This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would have recognized that use of Mastrovito standard-basis multiplier

would have provided the opportunity to implement a composite-basis multiplier with reduced complexity and higher speed (lines 16-18 of page 31 of the Applicant's specification).

9. Claims 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, Yen-Hao (US 6571368 B1) and Mastrovito (Mastrovito, "VLSI designs for multiplication over finite fields GF(2.sup.m)," Int'l Conf. on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, 297-309, Rome, July 1988).

35 U.S.C. 103(a) rejection of claims 11-14.

Chen and Mastrovito substantially teach the claimed invention described in claims 1-3 and 10 (as rejected above).

However Chen and Mastrovito, does not explicitly teach the specific use of specific circuit components to implement binary operations for Galois Field multiplication.

The Examiner asserts that it would be an obvious engineering design choice to select specific circuit components to implement binary operations since that is what they are designed for.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Chen and Mastrovito by including use of specific circuit components to implement binary operations for Galois Field multiplication. This modification would have been obvious to one of ordinary skill in the art, at the time the invention was made, because one of ordinary skill in the art would

have recognized that use of specific circuit components to implement binary operations for Galois Field multiplication would provide the opportunity to implement binary operations for Galois Field multiplication based on obvious engineering design choice since that is what they are designed for.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph D. Torres whose telephone number is (703) 308-7066. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (703) 305-9595. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)-746-7240.

Joseph D. Torres, PhD
Art Unit 2133